The Importance of Network Standards

Having been in technology for 20+ years, I have been fortunate to have worked with some incredibly bright engineers, both on my team and as clients. I don't claim to be the sharpest engineer ever but I have a talent in recognizing differences and commonalities.

I believe network standards are critical, since no organization has unlimited time or money. Standardization leads to some important advantages, including:

- Cost savings, because very similar devices are easier to maintain and manage.
- Efficiency, as design and troubleshooting are easier.
- Improved security and high availability, since you have fewer variables to consider.

For all these reasons, executives should take personal ownership to make sure their technology adheres to some degree of standardization.

You don't have to be a technologist to understand the value of standardization. You probably have salespeople turning quotes in a specific fashion, your accounting person follows a standardized chart of accounts, your warehouse receives product and must inventory in a structured way, and you probably have operating procedures for the most critical parts of your business.

Non-technical? Here's where to start:

Many first time network administrators and desktop people try to first build out a network and *then* at some point, 5 or 10 years down the road, might try to create a network map.

Building a network is a lot like building a house. It makes more sense to create a logical network map *first*, identifying the key pieces of your infrastructure that you will eventually build on.

THE FULCRUM GROUP
One Technology Solution: Yours

The Fulcrum Group, Inc. 5751 Kroger Drive, Suite 279, Fort Worth, TX 76244
Phone: 817.337.0300 Fax: 817.337.0313 Help Desk: 817.898.1277
info@fulcrumgroup.net www.fulcrum.pro

In the same manner, you build your foundation (cabling and physical plan), put up your walls (local area network), add on the roof (firewall) and buildout your rooms (servers and data repositories), all in a specific order.

If you are an executive managing an IT person or organization, your first step in managing them should be to ask them to map out the network so you can understand it visually.

My degree is in business but I found I could understand any technology by mapping it out visually, or outlining steps or implications. Eventually I became technical but also brought an operations manager mentality to understand technology.

If your IT person or vendor does not have a network map this could be a red flag.

You could also assist your technology provider by taking it upon yourself to map out your business critical processes. Identifying critical processes, process owners and workflow is a recommended activity in business management frameworks such as mentioned in Verne Harnish's Scaling Up.

If I'm a new IT guy and you show me your workflows, I can trace back to understand which systems are needed for these processes. It would help me understand where to invest limited budget first, or to think about high availability and drive innovation that should impact your bottom line.

Organize your list of assets for security and improved budgeting.
Before you can make decisions about your devices and security, you have to know what you have.

The ability to identify and manage network attached devices is very basic but requires the understanding needed to manage your technology.

- Simple asset lists in Excel are acceptable but there are variety of network management tools that can maintain an updated database of all assets for ready inspection.

- Having a list with the date in service or warranty expiration also helps you plan out equipment refresh or replacement with less fear of getting caught off guard with large unbudgeted costs.
- Management tools can also determine which devices on your network may be unauthorized. If someone simply put a wireless access point plugged into a network jack, they could bypass your firewall and attempt to connect to anything outside your front door and you might never know. Without appropriate management, if you've inventoried all of your authorized devices and one does not show up for a while, it could be lost and you wouldn't be aware.

Inventory and maintain your software, everyone benefits.
There's a saying that goes, "computer people are worried about the hardware and end-users are worried about the software."

Computer people spend much of their lives troubleshooting *hardware*. Replacing hardware and generally doing stuff that requires them to spend much of the day with hardware. So sometimes it is hard to change gears and realize that end-users may only replace their hardware once or twice but have to work within their *software* much of every single day.

Management should make sure that the support team has a complete list of every piece of software used on the network. That list should include what it's used for, who the information owner is, which users and groups should have access, any special permissions these people need, what version is being used and perhaps what patches or updates need to be applied. With the growth of Internet browser access to applications, it is harder to determine whether key applications are on the network or in the cloud.

Depending on the specific application, it could be important to know where the data for the application is stored. There is a network axiom that you should always locate your users as close to their data as possible. Knowing where the data is stored can help improve end-user performance in accessing that data.

The rise of ransomware might also mean it is important to know where the data is to properly back it up and protect it. In 2013, Forbes magazine estimated that roughly 60% of small businesses close within six months of a cyber-attack.

In addition to backing up your data you might want to look at the process of encryption to protect your data from unwanted access. Encryption is a technical process designed to protect messages or information so that only authorized parties can read it. The process of protecting information via encryption dates back thousands of years to old Egypt. Caesars' and the Romans' as well as the Nazis' use of the Enigma machine are other notable examples along the way of protecting data.

Sometimes there are users who are using nonstandard applications that the whole organization might benefit from. If Joe is using a PDF writer to help make sure proposals have a certain look, it probably makes sense for Jim and Betty to also have access to a good PDF writer. Unfortunately, we find many times in small organizations that it is up to individual users to find great ideas on their own instead of IT being aware of all the great tools in use on the network.

Standardize your device-naming for improved management. The value of standardizing your device names relates to making it easier to update, manage and troubleshoot issues from a central location. There are standard processes in computers such as centralized updating, centralized policy push out, centralized management that benefit you by knowing exactly what device is where.

If your IT team has chosen to name your workstation after the serial number (which is a Dell default setting) you might ask them why that is, or perhaps investigate a better choice for naming. There could be other reasons why it is named that way but we've found great benefits in knowing who is using the device and making more meaningful names, such as:

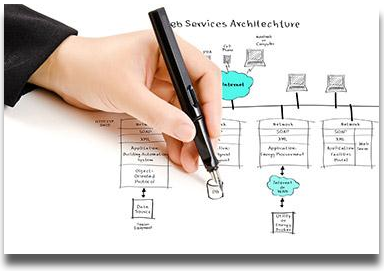
- Prefix desktops with DT (ex., DT-JDOE, DT-SALES1)
- Prefix laptops with LT (ex., LT-JDOE, LT-SALES1)
- Prefix tablets with TAB (ex., TAB-JDOE, TAB-SALES1)
- Prefix printers with PTR (ex., PTR-HP680, PTR-COPIER1)

THE FULCRUM GROUP
One Technology Solution: Yours

The Fulcrum Group, Inc. 5751 Kroger Drive, Suite 279, Fort Worth, TX 76244
Phone: 817.337.0300 Fax: 817.337.0313 Help Desk: 817.898.1277
info@fulcrumgroup.net www.fulcrum.pro

- Prefix servers with SVR (ex., SVR-DC, SVR-FORTWORTH)

The reason we've chosen the device type prefix is that depending on the device type, we might manage it using different - or similar - tools and policies. Depending on your organizational need you might choose to have a different suffix such as location, the username or the user's role (which might be a better fit for highly standardized users like a call center, local government or high turnover environments).



Group like-devices into smaller network address ranges. When designing a business network, it is also recommended to standardize the IP addresses used by the network with similar devices in like-ranges. Having similar devices grouped together also makes it easier to manage and maintain those assets. IP addresses are kind of like phone numbers for computer devices. They let each device know how to communicate with each other. Usually servers, firewalls, switches and other centrally utilized resources have their address statically configured by an administrator.

Additionally, Dynamic Host Configuration Protocol (DHCP) is a service you can run in your network to automate the handing out of IP addresses to people accessing resources. This allows the user to plug their computer into the network and have it automatically know how to talk to everything else on the network. The DHCP service tells the computer how to get outside the network to access the Internet, and also how to reach other resources on the network. DHCP also provides other information that might be helpful, such as a voice over IP phone grabbing the configuration.

A typical small business network might have a maximum of 254 addresses within its usable range. A sample structure for organizations mapping out addresses could look something like the structure below:

- .1 Default gateway (firewall/router)
- .2-.9 Infrastructure (switches, wireless, WLAN controller)
- .10-.19 Other devices (NAS, SAN, UPS, PDU, KVM)
- .20-.39 Printers/copiers/fax

- .40-.49 Security devices (IDS/IPS, email filter, web filter,
- .50-.99 Standard DHCP range (automatically hands out addresses to end users)
- .100-.109 Hypervisor hosts/management (VMware or Hyper-V)
- .150-.169 Remote access range (remote users)
- .200-.209 Building, HVAC, elevator, alarm
- .210-.239 Server IPs (file, mail, database, application, terminal)

The separation of devices facilitates the ability to limit or expand capabilities by knowing the device IPs on the network.

Draft IT policy and standardize configurations.

When I speak with larger organizations about technology, we typically refer to their existing IT policies. I find smaller businesses feel that IT policies send a message to their users that they don't trust them, even though that is almost never the case.

IT policies are designed to assist non-technical team members understand what right behavior looks like.

Most end-users want to do the right thing but without application or security awareness training, they don't know what they don't know.

Even a basic IT policy or some training can have a huge impact on end-users.

For administrators, standardized configuration could mean no device makes it on the network with the default password (there are huge lists of default passwords, making it easy to compromise them) or that no Windows system makes it on the network without windows patches and an updated antivirus software installed.

For end-users, standardized configuration could mean the administrator has configured Windows Group Policy to standardize settings such as screensavers, password lock out, mailbox settings or enhanced logging.

THE FULCRUM GROUP
One Technology Solution: Yours

The Fulcrum Group, Inc. 5751 Kroger Drive, Suite 279, Fort Worth, TX 76244
Phone: 817.337.0300 Fax: 817.337.0313 Help Desk: 817.898.1277
info@fulcrumgroup.net www.fulcrum.pro

Password policy could benefit from using complex characters, having a really long password or changing your password every 30 days. It is better to balance your password policy with your environment's users.
Forcing users to 8 characters, all complex characters, changed every 30 days might encourage users to use more Post-it notes on their workstation or change Password1 to Password2.

You might be better off encouraging users to 12 character passphrases, without complexity and changing every 60 days. It would probably be easier for users to remember a passphrase such as "IShallCallHimSquishy" or "LiveLongAndProsper1" without writing it down.

Summary
Without getting overly technical, my aim with this document is to help an executive or manager with a packed-full schedule have a better start at knowing and managing their technology environment.

Use the above six areas of discussion to cultivate an understanding of your comfort-factor within a technology capability model. Without some success in these six areas, you will struggle to grow your organization's technology to the next level.

A network administrator should read this information and try to determine where they can be most impactful with the information in this document.

The project manager in me looks for opportunity areas that will yield the biggest results, or areas that are easy fixes. The sooner you can reap some benefits, the more time you'll have to work on the next item.

For owners and managers where technology is a key part of your businesses' competitive advantage, you need to stop now and make the commitment to do something different. This could be directly managing IT differently, sending your IT administrator out for training, adding a more CIO-level technologist to your team, replacing your current IT person/provider or consider outsourcing your technology. But just like the oft-touted definition of insanity, things won't change until you do.

THE FULCRUM GROUP
One Technology Solution: Yours

The Fulcrum Group, Inc. 5751 Kroger Drive, Suite 279, Fort Worth, TX 76244
Phone: 817.337.0300 Fax: 817.337.0313 Help Desk: 817.898.1277
info@fulcrumgroup.net www.fulcrum.pro